

This week there was a variety of interesting items in the world of HIPAA. I hope you find the enclosed information to be of interest. Also, my thanks to all who contributed information!!!

Remember, it is important to take steps now to address HIPAA so that on October 16, 2002, you won't be saying "I'm in a HIPAA trouble!!!"

Please be sure to note that in some cases the information presented may be the opinion of the original author. We need to be sure to view it in the context of our own organizations and environment. In some cases you may need legal opinions and/or decision documentation when interpreting the rules.

Have a great day!!!
Ken

Topics included below are:

- WEDI's Privacy Rule Implementation Specifications & documents
- WEDI SNIP Forum on HIPAA Implementation (see attachment)
- [hipaalive] PRIVACY: Confidentiality - State Law Lists - CA
- [hipaalive] GENERAL: Compliance regarding faxing
- [hipaalive] PRIVACY: EOB
- [hipaalive] Security: Business Associates
- [hipaalive] GEN: State Medicaid
- [hipaalive] TRANSACTIONS compared to HCFA Form
- HIPAAcomply - Recent Federal Legislation
- [hipaalive] GENERAL: PHYSICAL NETWORK MANAGEMENT SOFTWARE
- Microsoft, HIPAA-Assessment, Remediation Implementation & Tools presentation (see attachment)
- HIPAAALERT - lite

***** WEDI's Privacy Rule Implementation Specifications

WEDI has a document on HIPAA Privacy Final Rule Table that gives the "Standard" and the corresponding "Implementation Specifications". It can be found at:
http://www.wedi.org/snip/presentations/SNIP_Forum/Privacetable.pdf
This is interesting as some of the penalties are related to "standards" not met, and there seems to be quite a lot of standards listed.

WEDI also has some definitions at -
http://www.wedi.org/snip/presentations/SNIP_Forum/FinalRule_Definitions.pdf
and a Glossary at:
http://WWW.WEDI.ORG/public/articles/HIPAA_GLOSSARY.pdf

***** [hipaalive] PRIVACY: Confidentiality - State Law Lists

from: Sjohnson@dmhq.state.ca.us

*** This is HIPAAlive! From Phoenix Health Systems ***

The Health Privacy Project at Georgetown University has compiled an extensive list of state laws. Go to: www.healthprivacy.org/ and click on the State Laws button. You can get California laws as well as other states.

NOTE: The direct address for CA information is:
www.healthprivacy.org/usr_doc/34034%2Epdf

*** This is HIPAAlive! From Phoenix Health Systems ***

California's general medical information confidentiality law begins at Civil Code section 56. There are special provisions relating to information about mental health and developmental disabilities in the Lanterman-Petris-Short Act (Welfare & Institutions Code section 5328) and the Lanterman Developmental Disabilities Services Act (W & I Code section 4514). For special provisions relating to certain drug and alcohol abuse programs, see Health and Safety Code sections 11812, 11977 and 11878.

Paul T. Smith
Davis Wright Tremaine LLP

*** This is HIPAAlive! From Phoenix Health Systems ***

The California Confidentiality of Medical Information Act of 1984, amended in 2000, covers general patient identifiable medical information for most all cases and exceptions. Patient identifiable medical information that contains HIV/AIDS status, mental health and substance abuse are further restricted and defined by federal law.

G. Adrian Cooley, RHIA
Health Services Information Systems Specialist
Contra Costa Health Services Information Systems

***** [hipaalive] GENERAL: Compliance regarding faxing

*** This is HIPAAlive! From Phoenix Health Systems ***

Faxed documents would be covered under the Privacy Rule. We have established a policy and developed templates to address faxing of identifiable health information. This includes situations when the faxed document is generated by an application.

The policy includes:

- * Verification of recipient
- * Procedure when fax (incoming and outgoing) is misrouted
- * Placement of fax machines and how frequently they need to be checked
- * A boilerplate fax cover with confidentiality language
- * The types of material that can be faxed and under what circumstances
- * Etc.

I think it is a good idea to establish a solid practice with associated polices to protect the sender and recipient. Faxed documents, today, aren't covered under the data security NPRM but are covered under the Privacy Rule. The Privacy Rule includes language that, for the most part, mandates solid data security. In addition, I think it is sound business practice as well as good stewardship to make sure faxed documents are treated with the care that would be associated with other transmitted identifiable health information.

Chris Apgar,
Data Security & HIPAA Compliance Officer
Providence Health Plan

***** [hipaalive] PRIVACY: EOB *****

*** This is HIPAAlive! From Phoenix Health Systems ***

This is still being somewhat hotly debated. Our counsel's opinion is including identifiable health information for someone other than the subscriber on an explanation of benefits (EOB) sent to the subscriber would be a violation of the HIPAA Privacy Rule. Per counsel, it also appears to be a violation of Oregon statute.

It can possibly be argued that such release is permissible because it is related to payment. On the other hand, I think it can also be argued that, while the subscriber may have a right to information about claims payments made, he or she does not have the right to have access to identifiable information about diagnosis, provider credentials, etc. ("need to know" is lacking).

I know some plans send EOBs to the member while others continue to send it to the subscriber with identifiable information. The debate goes on...

Chris Apgar,
Data Security & HIPAA Compliance Officer
Providence Health Plan

-----Original Message-----

I seem to recall this question coming up on this list serve in the past, and now regret not paying attention. Perhaps some kind soul will fill me in.

Question: Do the privacy regs preclude a payer from sending an EOB (explanation of benefits) to a subscriber for services provided to other family members (spouse, children). The EOB would have the patient's name, provider of service and usually procedure codes and payment responsibility. Would just disclosing the visit itself to the subscriber without specific authorization from the actual member be a violation of the HIPAA disclosure requirements?

***** [hipaalive] Security: Business Associates *****

*** This is HIPAAlive! From Phoenix Health Systems ***

Although HIPAA does not directly control the business associate, covered entities will want to know that their business associates

have adequate "safeguards". Those safeguards include policies, procedures and other security mechanisms that are appropriate to protect the security of the PHI that the covered entity has entrusted to their business associate.

While the Privacy rule is clear that the Privacy rule is separate from the Security rule, it does give us some guidance as to the security required for a business associate.

- 1) The safeguards required by a covered entity of a business associate are found in Sec. 164.504(e)(2)(ii)(B), which requires the covered entity to contractually ensure that their business associate uses appropriate safeguards to prevent use or disclosure of the information other than what is provided for in the business associate contract.
- 2) The safeguards required of a business associate should parallel those required of a covered entity under Sec. 164.530(c)(2), "A covered entity must reasonably safeguard protected health information from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements of this subpart..."
- 3) See FR Pages 82745-6 for HHS comments on safeguards and FR Pages 82503-4 for commentary related to safeguards, including examples of appropriate safeguards.
- 4) Note: There is no requirement for a covered entity to audit their business associate to determine if they are providing adequate safeguards. A covered entity's requirement to ensure that their business associate's provide adequate safeguards could be met if their business associate were to attest they were organizationally compliant to the Security rule (when final).

Thanks,

Tom Hanks
37W542 High Point Court

***** [hipaalive] GEN: State Medicaid *****
*** This is HIPAAlive! From Phoenix Health Systems ***

Oregon's Medicaid Office has been working with the transactions and code sets rules since July 2000, and has completed a gap analysis. The impact of these rules on State Medicaid Offices is obvious and extensive, and Medicaid Offices are clearly defined as Health Plans under HIPAA. But for other agencies in the Department of Human Services such as child protection, welfare, health division, vocational rehabilitation, senior services, mental health, and alcohol/drug services the impact is not as easily defined. Have any of you designed a Transaction/Code Sets impact assessment for state human service agencies other than Medicaid? How have you directed non-Medicaid agencies to determine how and to what extent the Transaction and Code Sets Rule impacts their agency? Looking forward to your responses.

Jane Alm, Oregon Medicaid Office

***** [hipaalive] TRANSACTIONS compared to HCFA Form *****
*** This is HIPAAlive! From Phoenix Health Systems ***

Most of these "mandatory" elements are either constant, or almost constant. I know of three instances:

- Provider Taxonomy Code (provider specialty) is not on the paper form, but in general is practically constant, or the provider can create a lookup table based on TaxID, name, or another field.
- Claim Sequence Indicator (whether the payer on this claim is Primary, Secondary, or Tertiary) is sometimes represented on the paper form on a non-standard way, like using "P" or "S" or "T" instead of "X" on the check boxes at the top, or the word "primary" somewhere on the claim.
- Several X12 data qualifiers. These are X12 semantic elements that indicate whether a number is a SSN or a TaxID, or whether a number is a telephone number or a fax number. In general these are set in your translator map and never change, but your translator can make these change as appropriate.

Other than these three, there are some elements that are used under defined "situations", such as DME certifications, and you probably would not even consider using a 1500 form for those anyhow. If you bill an unusual type of claim, you need to look at these "situational" elements, and see what you need under HIPAA as opposed to what you are doing today.

This is part of your "gap analysis". I would recommend you look at the implementation guides very carefully. Downloadable from [//hipaa.wpc-edi.com/](http://hipaa.wpc-edi.com/)

I hope this helps.

Kepa Zubeldia
Claredi

There are dozens of data elements in the 837 standard that are not currently being captured by most systems. Comparing what fields are currently required with what 837 requires is commonly called a cross-walk. Although the cross-walk for UB-92 does not seem to be done, you can see the cross-walk for the 1500 compared to 837 - Professional on the AFEHCT web site. Go to afehct.org, and look under ASPIRE. Since these are electronic standards, there is no new form.

***** HIPAAcomply - Recent Federal Legislation *****
Arizona Rep. introduces new HIPAA Legislation

Health Data Management (May 30, 2001)

Rep. John Shadegg (R-Ariz.) has introduced legislation to establish uniform, delayed compliance dates for most of the HIPAA administrative simplification provisions. The bill, H.R. 1975, is similar to legislation Sen. Larry Craig previously introduced in the Senate. Craig on May 25 considered pulling his bill from committee and putting it on the Senate floor for immediate action, but could not muster enough support.

Posted to HIPAAcomply 5/30/01

Bill to delay HIPAA still in Committee
Health Data Management (May 29, 2001)

Efforts on May 25 to bring HIPAA legislation to the Senate floor for an immediate vote failed and the bill remains in the Finance Committee. The bill, S. 836, sets an October 16, 2004 compliance date for HIPAA rules governing transactions/code sets, data security and provider and payer identifiers; or two years after the final rules are adopted and reliable provider and payer identifiers are available, whichever is later. The American Medical Association, American Public Human Services Association and Blue Cross and Blue Shield Association requested the legislation.

Posted to HIPAAcomply 5/29/01

Source is: www.hipaacomply.com

***** [hipaalive] GENERAL: PHYSICAL NETWORK MANAGEMENT SOFTWARE

*** This is HIPAAlive! From Phoenix Health Systems ***

Layer 1 is the Physical Layer (the wire or cable)
Layer 2 is the Data Link Layer (where non-routable protocols live)
Layer 3 is the Network Layer (where routable protocols like TCP/IP live)

There are 4 additional layers:
4 is the Transport Layer
5 is the Session Layer
6 is the Presentation Layer
7 is the Application Layer

All together they make up the Open Systems Interconnection (OSI) Model - a networking framework standardizing how protocols operate. Basic operation is that a node(A)

passes information beginning at the Application layer down through all layers to layer 1, where the data is placed in a packet that is sent along a wire to node(B). The data is passed up through all layers of the stack to the Application layer on node(B).

That probably was too much detail, but, I think you will get the general idea.

Regards,

Michael D. Tonick, CISSP
Manager KPMG Consulting - HIPAA Practice

***** HIPAA ALERT - lite *****

>>> <info@phoenixhealth.com> 05/29/01 08:20AM >>>

=====

May 29, 2001

>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
> Healthcare IT Consulting & Outsourcing <

=====

Subscribe free at: <http://www.hipaadvisory.com/alert/>

=====

H I P A A n e w s

*** Democratic Senate Could Help Privacy Law, Observers Say ***

The U.S. Senate will be more likely to take a favorable view of privacy legislation when it comes under Democratic control, privacy advocates and observers said Friday. Several Democrats assuming key leadership posts have shown an interest in the privacy issue in the past.

<http://www.hipaadvisory.com/news/index.htm#dem0529>

*** AFEHCT Challenges Blues' Report on Cost of HIPAA Transactions ***

The Association for Electronic Health Care Transactions (AFEHCT) has published an annotated version of the recent Blue Cross/Blue Shield Association report, "Provider Cost of Complying with Standardized Electronic Formats." In the annotations, AFEHCT challenges the conclusion that a delay for compliance is required.

<http://www.hipaadvisory.com/news/2001/afehct0523.htm>

*** DHHS Lacks Staff ***

Key positions in the Department of Health and Human Services (DHHS) are unfilled due to the lengthy appointment process, according to a report in the Boston Herald. At Boston College commencement ceremonies last week, Sec. Thompson expressed frustration with the process, the paper stated.

*** Many Hospitals Not Ready for HIPAA ***

According to a report in Health Forum, 57% of hospitals responding to a recent AHA member survey said they are on track to meet the Oct. 16, 2002, HIPAA transactions deadline. The survey showed hospitals have taken a number of general steps to prepare for the compliance deadline, but fewer have engaged in more specific actions related to implementation and compliance.

<http://www.hipaadvisory.com/news/index.htm#ahaready>

=====

H I P A A l a t e s t

NEW IN HIPAAZINE:

- Quite quarrelsome: Provider advocates still argue against privacy rules now in effect, by Mary Chris Jaklevic

Even with federal rules now in effect to protect the privacy of medical records, some provider organizations haven't given up the fight to blunt the rules' impact.

<http://www.hipaadvisory.com/news/Hipaazine.htm#quarrel>

- Preliminary HIPAA compliance recommendations, by Andrea Kahn-Kothmann

A description of the statutory and regulatory context for the Privacy Standards, a brief overview of the rules, and several recommendations of practical steps for physicians.

<http://www.hipaadvisory.com/news/Hipaazine.htm#pnd0401>

NEW IN HIPAATECH:

- Application Service Provider Security Issues

<http://www.hipaadvisory.com/tech/aspsec.htm>

NEW IN HIPAAUDIO:

- Legally HIPAA! A Summer Audioconference Series with Steve Fox, Esq., author of HIPAAAdvisor

June 20: Handling Consents and Authorizations

July 18: Handling Chain of Trust & Business Associate

August 22: Developing Privacy/Security Policies and Procedures

<http://www.hipaadvisory.com/order/legal/index.cfm>

=====

HIPAAAlert-lite is our weekly version of HIPAAAlert, Phoenix Health Systems' acclaimed monthly email newsletter. HIPAAAlert-lite is published each Monday to keep subscribers abreast of breaking news and industry developments in healthcare privacy and security.

Our Other HIPAA resources:

Web site: <http://www.hipaadvisory.com>

Discussion List: <http://www.hipaadvisory.com/live/>
Weekly Awareness Note: <http://www.hipaadvisory.com/notes/>

=====

COMMENTS? Email us at info@phoenixhealth.com
SUBSCRIBE? Visit <http://www.hipaadvisory.com/alert/>
ARCHIVES: <http://www.hipaadvisory.com/alert/newsarchives.htm>

=====

Copyright 2001, Phoenix Health Systems, Inc. All Rights Reserved.
Reprint by permission only.
<http://www.phoenixhealth.com> 301-869-7300

=====

FORWARD this posting to interested associates, who may subscribe free to HIPAAAlert at:

<http://www.hipaadvisory.com/alert/>
Subscribe to our free discussion list at:
<http://www.hipaadvisory.com/live/>
Get a weekly byte of HIPAA at:
<http://www.hipaadvisory.com/notes/oording>
[to a report in the Bo](#)

You are currently subscribed to hipaalert as:kmckinst@dmhhq.state.ca.us
To unsubscribe send a blank email to leave-hipaalert-85079900@lists.hipaalert.com